MASTER OF SCIENCE
IN
COMPUTER SCIENCE

REAL-TIME MODELING OF CROSS-BODY FLOW FOR TORPEDO TUBE RECOVERY OF THE *PHOENIX* AUTONOMOUS UNDERWATER VEHICLE (AUV)

Kevin Michael Byrne-Lieutenant, United States Navy
B.S., State University of New York Maritime College, 1991
Master of Science in Computer Science-March 1998
Advisor: Don Brutzman, Undersea Warfare Academic Group
Second Reader: Robert P. McGhee, Department of Computer Science

A virtual world provides an exceptional resource for the testing and development of an Autonomous Underwater Vehicle (AUV). The difficulties associated with the underwater environment are numerous and complex. In order to properly verify vehicle results in the laboratory such a world must accurately model the physics associated with the vehicle, its submerged hydrodynamics characteristics, and interactions with the environment. Environmental effects such as wave motion, currents, and flow forces created by bodies moving through the water can cause unpredicted performance variations and failures in the ocean environment. The current *Phoenix* AUV virtual world includes steady-state ocean currents, but does not take into account the environmental effects of waves and flow forces induced by adjacent vehicles (such as a moving submarine docking target).

This work provides a thorough real-time simulation of these complex factors using physically-based models. The problem is broken down into wave motion effects, submarine-induced flow fields, and virtual sensors to improve AUV motion control. Each set of forces is thoroughly analyzed and realistically simulated in real-time through the algorithms developed. In order to maintain real-time response, perturbations in the flow field caused by the AUV itself are assumed to be negligible. Simulated testing is performed across a range of easy to worst-case scenarios in order to justify assumptions. Extensive testing using virtual sensors is used to develop adequate control algorithms in the presence of turbulent cross-body flow.

The result of this research is an enhanced virtual world which more accurately depicts the ocean environment, along with the models and control algorithms required to design and operate an AUV during submarine launch and recovery. A platform independent approach to virtual environment simulation is presented through the use of the Virtual Reality Modeling Language (VRML) and Java. Finally, simulation test results provide strong evidence that AUV control with actual cross-body flow sensors can enable stable navigation, first through a turbulent flow field and then for subsequent docking with a moving submarine.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Surface/Under Surface Vehicles - Ships and Watercraft, Modeling and Simulation

KEYWORDS: Virtual Environment, Simulation-Based Design, Cross-Body Flow, Autonomous Underwater Vehicle (AUV), Platform-Independent Simulation

---

MASTER OF SCIENCE IN COMPUTER SCIENCE

A STATIC SECURE FLOW ANALYZER FOR A SUBSET OF JAVA

James D. Harvey-Lieutenant, United States Navy
B.S., Ohio State University, 1990
Master of Science in Computer Science-March 1998
Advisor: Dennis M. Volpano, Department of Computer Science
Second Reader: Craig W. Rasmussen, Department of Mathematics

As the number of computers and computer systems in existence has grown over the past few decades, we have come to depend on them to maintain the security of private or sensitive information. The execution of a program may cause leaks of private or sensitive information from the computer. Static secure flow analysis is an attempt to detect these leaks prior to program execution.

It is possible to analyze programs by hand, but this is often impractical for large programs. A better approach is to automate the analysis; which is what this thesis explores.

Previous research is described and gives background information about secure flow analysis. A secure flow analyzer is presented. It implements a secure flow type inference algorithm, for a subset of Java 1.0.2, using a parser generator called Java Compiler Compiler (JavaCC). Semantic actions are inserted into a grammar specification to perform the secure flow analysis on a given program.

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: Secure Flow Analysis, Type Inference, Program Certification, Information Flow, Protection

THE DESIGN AND IMPLEMENTATION OF THE PETITE AMATEUR NAVY SATELLITE (PANSAT) USER SERVICES SOFTWARE

George Kenneth Hunter-Lieutenant, United States Navy
B.S., United States Naval Academy, 1990
Master of Science in Computer Science-March 1998
Advisor: Man-Tak Shing, Department of Computer Science
Second Reader: James A. Horning, Space Systems Academic Group

PANSAT is an experimental spread spectrum, store-and-forward communications micro satellite. The Chief of Naval Operations C^4I staff (N6) sponsors the project in order to determine the feasibility and effectiveness of using such a low-cost satellite to augment or eventually replace the existing military satellite communications architecture. While more than eight years of work has gone into the project, most of the fifty theses thus far have dealt with hardware development. Prior to this thesis, the operations of the satellite were not formally defined, nor the desired software experiments specified.

This thesis develops a detailed definition of the communications software and operating parameters for PANSAT. The formally specified communications software provides electronic mail, binary file transfer, and direct real-time information exchange. This research also designs and develops experimental features which are non-existent on current micro satellites. The new features included provide the spacecraft with a pseudo positional awareness for a system with no sensor support for such, implement a new application layer protocol to optimize data communications, and perform self analysis to find and correct the effects of space anomalies in conjunction with a ground station.

This thesis also implements a subset of the formally specified software for initial operations to begin with spacecraft's launch in October of 1998. Further implementation and refinement will be based on actual operational results from PANSAT.

DoD KEY TECHNOLOGY AREAS: Space Vehicles, Command, Control, and Communications, Computing and Software

KEYWORDS: PANSAT, User Services, Spacecraft Engineering, Amateur Satellite Communications, Amateur Radio Service, Ground Station, Software Engineering, Fault Tolerance

SOFTWARE SYSTEM REQUIREMENTS FOR THE FUEL AUTOMATED SUBSYSTEM OF THE INTEGRATED COMBAT SERVICE SUPPORT SYSTEM (1C53) USING THE COMPUTER-AIDED PROTOTYPING SYSTEM (CAPS)

Lawrence A. Kominiak-Major, United States Army
B.S., United States Military Academy, 1987
Master of Science in Computer Science-March 1998
Advisor: Luqi, Department of Computer Science
Second Reader: Valdis Berzins, Department of Computer Science

The United States Army is currently developing and testing Force XXI, an attempt to redesign itself by the early years of the 21st century to incorporate digital technology and advanced weaponry. In 1996, the United States Training and Doctrine Command mandated that all combat service support disciplines be automated to the greatest extent possible. Concurrently, the Deputy Chief of Staff for Logistics, United States Materiel Command, and the Combined Arms Support Command (CASCOM) developed a future strategic vision of seamless logistics support. To support this vision, CASCOM has proposed the implementation of the Integrated Combat Service Support System (1C53) as the Army's single seamless combat service support management system. 1C53 will be a "system of systems" that automates the combat service support disciplines of man, arm, fuel, fix, move, and sustain. Specifically, the combat service support discipline of fuel will be incorporated in 1C53 as the Fuel Automated Subsystem.

This thesis analyzes current Army petroleum operations, identifies petroleum accountability/management procedures as the target domain for automation, and develops the respective software system requirements. From the software system requirements, a prototype for the Fuel Automated Subsystem is successfully developed using the Computer-Aided Prototyping System (CAPS) to illustrate the system's viability.

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: CAPS, Systems Analysis, Software Requirements, Prototyping, 1C53, Fuel Automated Subsystem

SECURITY ISSUES FOR THE SOFTWARE EVOLUTION MODEL

Anastasios X. Rambidis-Lieutenant, Hellenic Navy
B.S., Hellenic Naval Academy, 1987
Master of Science in Computer Science-March 1998
Advisors: Bert Lundy, Department of Computer Science
Luqi, Department of Computer Science

This thesis examines the security requirements of the software evolution model and identifies possible security mechanisms called "control classes" that are applicable to the model. Then, based on combinations of "control classes," proposes a suitable security level for each of the model's databases. Furthermore, this thesis deals with the possibility of using Pretty Good Privacy as a method for protection of software data stored in databases**.**

The software evolution model captures all the necessary changes in requirements early during the development process in order to help in minimization of project cancellation, delivery delays, and extra costs for fixing errors. The protection of software data against unauthorized accesses and modifications is a primary consideration for the software evolution process. In this way, we can develop a secure environment on which the software evolution can rely for accomplishing its goal.

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: Database Security, Software Evolution, Software Data Security, Pretty Good Privacy, Data Encryption/ Decryption

AN ENTERPRISE INFORMATION SYSTEM FOR THE NAVAL SECURITY GROUP

James V. Stevenson-Lieutenant Commander, United States Navy
B.A., Eastern New Mexico University, 1987
Master of Science in Computer Science-March 1998
Advisor: C. Thomas Wu, Department of Computer Science
Second Reader: Gus Lott, Department of Electrical and Computer Engineering

U.S. Naval Security Group (NSG) community data resides in disassociated systems with no clear data hierarchy. The NSG's lack of a central information framework wastes money, consumes manpower, and underutilizes claimancy resources.

To improve NSG data operations, an Enterprise Information System (EIS) was designed and implemented using Commercial-Off-The-Shelf hardware and software. First, an Internet browser-based, client-server architecture was selected that optimizes performance, interoperability, and cost. Next, a database schema was designed and instantiated using relational technology. Then, web server database access files were created that emphasize connectivity and utility. Finally, EIS integrity and privacy concerns were examined.

The prototype NSG EIS optimizes personnel and resources, improves data accuracy and timeliness, and enhances the Naval Security Group's aggressive pursuit of information dominance. The proposed EIS provides the NSG with an affordable and efficient method for bringing timely and accurate information to bear in an increasingly information dependent military.

DoD KEY TECHNOLOGY AREAS: Command, Control, and Communications, Computing and Software

KEYWORDS: Database, Enterprise Information System, Naval Security Group, SQL Server

AN APPROACH TO MOBILE AGENT SECURITY IN JAVA

Roy John Virden-Lieutenant, United States Navy
B.A., Miami University, 1990
Master of Science in Computer Science-March 1998
Advisor: Dennis M. Volpano, Department of Computer Science
Second Reader: Nelson D. Ludlow, U.S. Air Force Radar Evaluation Squadron

For many years, people have talked about the advantages of programs that can roam networks and provide services for a client. The programs, called agents, have many military applications as well. Among them, for instance, is data mining, where an agent is dispatched to find information for a client.

There are security risks associated with agents. For instance, in the data mining example, a client must be able to trust the information returned. If a trusted node in a network can be spoofed, then an untrusted node can easily corrupt the results of the mining operation.

This thesis presents a protocol to guard against this sort of attack. The protocol assumes that every trusted host knows all other trusted hosts. Though unrealistic for some commercial applications, it seems like a reasonable assumption for military applications.

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: Mobile Agent, Security, Java, Authentication Protocol